REMARKS

Applicants appreciate the thorough review of the present application as reflected in the Official Action mailed May 7, 2004. However, Applicants submit that the present application is patentable over the cited references as the cited references do not disclose or suggest each of the recitations of the pending claims.

Applicants have amended the specification to provide the serial number of the related application and have cancelled the non-elected claims. Applicants have also amended Claims 2 and 40 to write these claims in independent form and have cancelled Claims 1 and 39.

The IDS

Applicants wish to bring to the Examiner's attention an IDS that is being submitted concurrently herewith. Applicants request that an initialed copy of the PTO-1449 form be returned with any subsequent communication.

The Restriction Requirement

In response to the Restriction Requirement, Applicants confirm the election of Invention I, corresponding to Claims 1-57 and 77. Applicants have canceled Claims 58-76, 78 and 79 corresponding to Invention II. This cancellation is being made without prejudice to the filing of any divisional applications for these and/or other claims. This election is without traverse because Applicants agree that a determination of the unpatentability of Invention I would not necessarily imply the unpatentability of Invention II.

The Section 112 Rejections

Claims 21 and 36-38 stand rejected under 35 U.S.C. § 112, second paragraph, for failing to particularly point out and distinctly claim the subject matter which applicant regards as his invention. Official Action, p. 3. In particular, Claim 21 is rejected as the recitation "rules information" does not have proper antecedent basis. Applicants have amended the dependency of Claim 21 to depend from Claim 20 to provide the proper antecedent basis. Claim 36 is also rejected as being self dependent and Claims 37 and 38 are rejected as being dependent on a rejected base claim. Applicants have amended the dependency of Claim 36 so that Claim 36 depends from Claim 28.

In light of the above discussion, Applicants submit that the rejection of Claims 21 and 36-38 under 35 U.S.C. § 112 has been overcome.

The Claims Are Not Anticipated

Claims 22 and 27 stand rejected under 35 U.S.C. § 102(b) as anticipated by United States Patent No. 5,022,077 to Bealkowski et al. (hereinafter "Bealkowski"). Official Action, p. 3. In rejecting Claims 22 and 27, the Official Action cites to col. 3, lines 10, 26 and 31 et. seq. of Bealkowski as disclosing the recitations of these claims. Official Action, p. 4. In particular, the paragraph that includes lines 26 and 31 of col. 3 of Bealkowski states:

> Broadly considered, a personal computer system according to the present invention comprises a system processor, a random access memory, a read only memory, and at least one direct access storage device. A direct access storage device controller coupled between the system processor and direct access storage device includes a means for protecting a region of the storage device. The protected region of the storage device includes a master boot record and a BIOS image. In response to a reset signal, the protection means permits access to the protected region to allow the master boot record to be loaded into random access memory. In operation, the master boot record further loads the BIOS image into random access memory. BIOS, now in random access memory, is executed and generates a second signal which activates the protection means to prevent access to the region on the disk containing the master boot record and the BIOS image. BIOS then boots up the operating system to begin operation of the system.

Bealkowski, col. 3, lines 18-37. Thus, the cited portion of Bealkowski describes a direct access storage device controller allows access to a master boot record and BIOS image after a reset signal and subsequently prevents access to a region of a disk containing the master boot record and the BIOS image.

Under 35 U.S.C. § 102, "a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." M.P.E.P. § 2131 (quoting *Verdegaal Bros. v. Union Oil Co.*, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987)). "The fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.'" M.P.E.P. § 2112 (citations omitted) (emphasis added).

A finding of anticipation further requires that there must be no difference between the claimed invention and the disclosure of the cited reference as viewed by one of ordinary skill in the art. *See Scripps Clinic & Research Foundation v. Genentech Inc.*, 18 U.S.P.Q.2d 1001 (Fed. Cir. 1991). Thus, anticipation requires that a single prior art reference disclose each and every element of the anticipated claim.

In contrast to the direct access storage device controller described in the cited portion of Bealkowski, Claim 22 recites:

> 22. (Original) A system for controlling access to a programmable memory of a device, comprising:
>
> a latch;
>
> a memory controller configured to control read and write operations to the programmable memory and operably associated with the latch so as to allow write operations to the programmable memory when the latch is in a first state and to prevent write operations to the programmable memory when the latch is in a second state;
>
> a latch enable circuit configured to set the latch to the first state upon detecting a hardware reset of the device and set the latch to the second state upon completion of a memory update window.

The cited portion of Bealkowski does not describe the latch recited in Claim 22. Furthermore, the cited portion of Bealkowski does not describe a memory controller responsive to a latch that controls read and write operations of a programmable memory as recited in Claim 22. Instead, Bealkowski describes controlling access to regions of a disk. The cited portion of Bealkowski does not describe the state of a latch controlling whether a programmable memory can be written to. Accordingly, Applicants submit that Claim 22 is not anticipated by Bealkowski. Analogous arguments apply to the read operations recited in Claim 27.

In light of the above discussion, Applicants submit that Claims 22 and 27 are not anticipated by Bealkowski as the cited portion of Bealkowski does not describe controlling read or write operations for a programmable memory by the state of a latch as recited in these claims.

The Claims Are Not Obvious

Claims 1-20, 39-57 and 77

Claims 1-20, 39-57 and 77 stand rejected as obvious in light of United States Patent No. 5,844,986 to Davis (hereinafter "Davis") in view of United States Patent No. 5,293,424 to Holtey *et al.* (hereinafter "Holtey"). Official Action, p. 5. Applicants have cancelled Claims 1 and 39 and, therefore, will discuss the rejection of independent Claims 2, 40 and 77. The remaining claims all depend, either directly or indirectly, from Claims 2, 40 or 77.

To establish a *prima facie* case of obviousness, the prior art reference or references when combined must teach or suggest *all* the recitations of the claims, and there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. *See* M.P.E.P. § 2143. The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *See* M.P.E.P. § 2143.01(citing *In re Mills* , 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990)). As emphasized by the Court of Appeals for the Federal Circuit, to support combining references, evidence of a suggestion, teaching, or motivation to combine must be **clear and particular**, and this requirement for clear and particular evidence is not met by broad and conclusory statements about the teachings of references. *In re Dembiczak*, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999). In another decision, the Court of Appeals for the Federal Circuit has stated that, to support combining or modifying references, there must be **particular** evidence from the prior art as to the reason the skilled artis an, with no knowledge of the claimed invention, would have selected these components for combination in the manner claimed. *In re Kotzab*, 55 U.S.P.Q.2d 1313, 1317 (Fed. Cir. 2000).

Furthermore, as recently stated by the Federal Circuit with regard to the selection and combination of references:

> This factual question of motivation is material to patentability, and could not be resolved on subjective belief and unknown authority. It is improper, in determining whether a person of ordinary skill would have been led to this combination of references, simply to "[use] that which the inventor taught against its teacher." W.L. Gore v. Garlock, Inc., 721 F.2d 1540, 1553, 220 USPQ 303, 312-13 (Fed. Cir. 1983). Thus the Board must not only assure that the requisite findings are made, based on evidence of record, but must also explain the reasoning by which the findings are deemed to support the agency's conclusion....

In re Sang Su Lee, 277 F.3d 1338, 1343 (Fed. Cir. 2002). Applicants submit that the Official Action has failed to establish a *prima facie* case of obviousness for the reasons discussed below.

In rejecting Claims 2, 40 and 77 the Official Action cites Davis, col. 4, line 14 as inherently disclosing "allowing access to the programmable memory based on the state of an access latch" as recited in these claims. Official Action, p. 5. It appears that the Official Action relies on general knowledge in asserting that "[a]ll BIOS functions take place after a hardware reset" and concludes that, therefore, the recitation of "setting the access latch to allow access to the programmable memory after a hardware reset of the device" of these claims is also in the prior art. Official Action, p. 6. The Official Action also cites to col. 2, lines 61 and col. 3, line 49 of Davis as disclosing the remaining portions of Claim 2. While no rationale is provided as to why Davis and Holtey would be combined to result in the recitations of Claim 2, Applicants assume that the same rationale would be applied as was applied in the rejection of Claim 1, namely that "utilizing additional security strategies helps to reduce potential security vulnerabilities." Official Action, p. 5.

While not stated in the Official Action, Applicants assume that the rejection of Claim 2 incorporates the rejection of Claim 1. In rejecting Claim 1, the Official Action cited to col. 5, line 55 of Holtey as disclosing the recitations of these claims. Davis does describe a secure update of BIOS but the security in Davis relates to the authenticity of the BIOS. *See* Davis, Abstract. Holtey describes a Secure Memory Card. *See* Holtey, Title. The cited portion of Holtey discusses a "reauthentication interval" which is an interval at which a user's identity is verified by the user having to enter a PIN or password. *See* Holtey, col. 5, lines 54-59. Holtey, however, describes the authentication process as allowing data to be read from memory. *See* Holtey, col. 3, lines 9-13.

In contrast to Davis and Holtey, Claim 2 recites:

> 2. (Currently Amended) A method of controlling updates of a programmable memory of a device, the method comprising:
>
> providing an update window of predefined duration during which the programmable memory may be updated; and
>
> allowing updates of the programmable memory only during the update window;
>
> wherein the steps of providing an update window and allowing updates comprise the steps of:

> allowing access to the programmable memory based on the state of an access latch;
>
> setting the access latch to allow access to the programmable memory after a hardware reset of the device;
>
> executing an update control program to control access to the programmable memory; and
>
> resetting the latch to prevent access to the programmable memory upon completion of the update control program.

Similar recitations are found in system Claim 40 and computer program product Claim 77. Neither Davis not Holtey describe using the state of an access latch to control access to a programmable memory. While the cited portions of Davis describe the selective application of a BIOS update based on authentication of the BIOS update, there is no indication the cited portions that access to a programmable memory is based on the state of a latch or even whether the update is authenticated. The application of the update may be controlled by the results of the authentication process but that does not necessarily mean that access to the memory is controlled by the results of the authentication process.

The Official Action's argument that "the validity variable used in '986 is stored in a memory latch, because this is the way by which computers process information" ignores the recitations of Claim 2 that the latch controls access to the programmable memory. *See* Official Action, p. 6. Applicants find no reference to a "validity variable" in the cited portions of Davis. In any event, as discussed above, the cited portions of Davis do not describe controlling access to a programmable memory but deciding whether to use a new BIOS version. *See* Davis, Fig. 3. Also, even if the validity variable is used only with the BIOS replacement operation in Davis as asserted by the Official Action at p. 6, that does not mean that mean that the variable controls access to a programmable memory or that it is reset "to prevent access to the programmable memory upon completion of the update control program" as recited in Claim 2.

The Official Action also makes unsupported assertions as to the prior art. *See* Official Action, p. 6. Applicants submit that an obviousness rejection cannot be based on unsupported assertions of what is known in the art. Applicants, therefore, request that, if the rejections are maintained, the Official Action support each assertion with a citation to a prior art reference.

Finally, the Official Action provides either no reason for combining Davis and Holtey in the manner recited in Claim 2 or, if the reasoning in the rejection of Claim 1 is applied, only an unsupported conclusory assertion. This type of conclusory assertion cannot be a proper basis for an obviousness rejection.

In light of the above discussion, Applicants submit that the Official Action has failed to establish a prima facie case of obviousness of Claims 2, 40 and 77 in that each of the recitations of the claims has not be found in the prior art references and no proper motivation to combine the references in the manner recited in the claims has been established. In fact, it is unclear to Applicants how the references are combined and how that combination would result in the recitations of Claims 2, 40 and 77. Accordingly, Applicants submit that Claims 2, 40 and 77 are patentable over the cited references.

While Applicants submit that the dependent claims are patentable as depending from a patentable base claim, Applicants submit that certain of the dependent claims are also separately patentable over the cited references. For example, Claims 3 and 41 recite "allowing access to a **memory where the update control program resides** when the access latch allows access to the programmable memory" and "preventing access to the **memory where the update control program resides** when the access latch prevents access to the programmable memory." There is no discussion in the cited portion of Davis of controlling access to the memory where the update control program resides as recited in Claims 3 and 41. The **authentication** is only with respect to the BIOS update. The Official Action's citations do not appear to address the specific language of Claims 3 and 41. Applicants request that the Examiner explain why the statement in Davis that "[i]f the new BIOS is valid, the new BIOS program is made operational and the previous BIOS program is deleted," and the statement that "[t]he authentication and validation are performed by a security processor which contains the BIOS firmware," which appear to be the only portions of Davis cited in the rejection, disclose controlling access to the memory where an update control program resides. *See* Davis, col. 4, lines 14-16 and col. 2, line 59 and Official Action, p. 6. Accordingly, Applicants submit that Claims 3 and 41 are separately patentable for at least these additional reasons.

Claims 20 and 56 each recite "obtaining application rules information from an extension of at least one certificate associated with the update" and "evaluating the rules information obtained from the at least one certificate." These claims further recite "selectively updating the programmable memory based on the evaluation of the rules information obtained from the at least one certificate." The Official Action cites to col. 4, line 27 and line 8 of Davis as disclosing the recitations of these claims. In particular, with respect to Claims 20 and 56, the Official Action cites to col. 4, line 27 and col. 4, line 8 of Davis as teaching the recitations of the claims regarding the application rules information. Official Action, p. 10. These cited portions of Davis appear to describe the standard use of a certificate to authenticate the source of a BIOS upgrade. *See* Davis, col. 4, lines 19-46. There is no mention of a certificate extension or rules for the application of an update being contained in a certificate extension.

The cited portion of Davis at col. 4, line 8 describes determining the validity of a new BIOS program. This validity determination appears to be based on the BIOS program itself, not based on rules provided in a certificate extension. For example, Davis states:

> Once the authentication operations have been performed, in step 160, the cryptographic coprocessor can make a determination as to the validity of the new BIOS program. For example, the digital signature supplied with the "new BIOS program" may be valid, but the revision date may be inappropriate (e.g. older than the currently installed BIOS). If the new BIOS is determined to be invalid, it is deleted by the cryptographic coprocessor and is never used (step 170). If the new BIOS is valid, the new BIOS program is made operational and the previous BIOS program is deleted (step 180). Note that at this point, it would be normal to reboot the computer system to assure system-wide consistency.

Davis, col. 4, lines 7-18. Thus, the only example of the determination that the "new BIOS" is invalid is the comparison of the revision date. There is no indication that any "update rules" are provided in an extension of a certificate as recited in Claims 20 and 56. In fact, the only mention of the certificate appears to be in connection with authentication. *See e.g.*, Davis, col. 3, line 63 to col. 4, line 4 and lines 19-46.

The cited portion of Davis at col. 4, line 27 also does not disclose or suggest the use of a certificate extension to provide update rules as recited in Claims 20 and 56. In particular, col. 4, line 27 of Davis appears to only provide further details regarding authentication. Thus, Davis states:

> To support this digital signature-based method of BIOS authentication, the digital signature embedded in the distribution BIOS software upgrade should be underwritten or endorsed by an industry association, or a similar organization or procedure. The participants in this industry association are the BIOS vendors who

> want to be able to field upgrade their BIOS code. One of the functions of this industry association is to issue digital certificates to its BIOS vendor members, essentially assigning a digital certificate to each vendor to be used in BIOS upgrade software. This association provides its public key to be used by the cryptographic coprocessor during the BIOS authentication procedure. The cryptographic coprocessor will be preloaded with the public key of the industry association for BIOS vendors so that it will be able to verify any digital signature embedded in the BIOS upgrade code. Alternatively, the cryptographic coprocessor may be preloaded with another public key that may be used to authenticate a certificate chain to obtain this industry association public key. The BIOS upgrade code could be encrypted if necessary (to protect the code from being reverse engineered for example). Since the digital signature or the certificate issued by the industry association normally represents the authenticity of a reputable or credible BIOS vendor, an intruder cannot corrupt the BIOS code (unless of course he or she somehow obtains secret private keys used to create such signatures or certificates) either directly or indirectly by virus attack.

Davis, col. 4, lines 19-46. This portion of Davis describes assigning a digital certificate to vendors for use in an authentication procedure, but there is no indication that an extension of the digital certificate is used to provide update rules or that update rules are provided at all.

In light of the above discussion, Applicants submit that each of the recitations of Claims 20 and 56 are not disclosed or suggested by the cited portions of Davis. Accordingly, Applicants submit that Claims 20 and 56 are separately patentable over the cited reference for at least these additional reasons.

Claims 23-26 and 28-35

Claims 23, 24 and 25 stand rejected under 35 U.S.C. § 103 as obvious in light of Bealkowski and United States Patent No. 5,579,522 to Christeson *et al.* (hereinafter "Christeson"). Claim 26 stands rejected under 35 U.S.C. § 103 as obvious in light of Bealkowski, Christeson and "Introduction to Digital Signal Processors." Claims 28-35 stand rejected under 35 U.S.C. § 103 as obvious in light of Bealkowski and Davis. Applicants submit that these claims are patentable at least as depending from a patentable base claim.

Conclusion

In light of the above discussion, Applicants submit that the present application is in condition for allowance, which action is respectfully requested.

It is not believed that an extension of time and/or additional fee(s)-including fees for net addition of claims-are required, beyond those that may otherwise be provided for in documents accompanying this paper. In the event, however, that an extension of time is necessary to allow consideration of this paper, such an extension is hereby petitioned under 37 C.F.R. §1.136(a). Any additional fees believed to be due in connection with this paper may be charged to our Deposit Account No. 09-0461.

Respectfully submitted,

Timothy J. O'Sullivan
Registration No. 35,632

Customer No. 20792
Myers Bigel Sibley & Sajovec
P. O. Box 37428
Raleigh, North Carolina 27627
Telephone: (919) 854-1400
Facsimile: (919) 854-1401